Bulletin of Electrical Engineering and Informatics
ISSN: 2302-9285
Vol. 6, No. 1, March 2017, pp. 99~104, DOI: 10.11591/eei.v6i1.599

Chaos Image Encryption Methods: A Survey Study

Sabah Fadhel[1*], Mohd Shafry[2], Omar Farook[3]
[1, 3]Faculty of Computing-Universiti Teknologi Malaysia (UTM), Skudai, Johor, Malaysia
[2]IRDA Digital Media Center, IHCE-Universiti Teknologi Malaysia (UTM)
Corresponding author, email: sabahuqaidy@yahoo.com

Abstract

With increasing dependence on communications over internet and networks, secure data transmission is coming under threat. One of the best solutions to ensure secure data transmissions is encryption. Multiple forms of data, such as text, audio, image, and video can be digitally transmitted, nowadays images being the most popular and old encryption techniques such as: AES, DES, RSA etc., show low security level when used for image encryption. This problem was resolved by using of chaos encryption which is an acceptable form of encryption for image data. The sensitivity to initial conditions and control parameters make chaos encryption suitable for image applications. This study discusses various chaos encryption techniques.

Keywords*: chaos, initial conditions, control parameters, map, permutation*

1. Introduction

Multimedia technology, especially image technology is currently undergoing rapid change and growth [6] due to increased adoption of internet communications [1]. Current encryption techniques, such as AES, DES, and RSA are unsuitable for image data encrypting and cannot guarantee data confidentiality and security [2] because of the size and redundancy of images [3-5]. Over the last couple of decades numerous techniques have been proposed for encrypting image data, of which Chaos based encryption has been proven to be the most effective [7]. Chaos theory was first proposed in the 1970's for use in physics, mathematics, biology and engineering. It would not be until the 1980's that chaos theory was found to have cryptographic applications [8]. Chaos based encryption methods are popular due to their randomness, unpredictability, sensitivity and topological transitivity [9-10].

Literature review that has been done author used in the chapter "Introduction" to explain the difference of the manuscript with other papers, that it is innovative, it are used in the chapter "Research Method" to describe the step of research and used in the chapter "Results and Discussion" to support the analysis of the results [2]. If the manuscript was written really have high originality, which proposed a new method or algorithm, the additional chapter after the "Introduction" chapter and before the "Research Method" chapter can be added to explain briefly the theory and/or the proposed method/algorithm [4].

2. Chaos Theory

A chaotic dynamical system is any deterministic system that is both highly random and sensitive to initial conditions [11]. Chaotic systems are similar to noisy systems because both are highly unpredictable. Chaotic systems have uses in cryptography because they are pseudorandom, unpredictable and sensitive to initial condition (starting point) and control parameters [1]. Chaotic systems are useful for encryption because they appear to be random data and their sensitivity to initial conditions allows for this randomness to be unpredicted, allowing a basis for decryption [12]. The main difference between chaos maps and chaos cryptography is that chaos cryptography is defined by finite sets, while chaos maps are defined by real numbers, as is shown in Table 1 [11]. Each chaos map has its own parameters and encryption key.

Received December 11, 2016; Revised February 11, 2017; Accepted February 25, 2017

Table 1. Illustrate the Differences and Similarities Between Chaotic System and Cryptography Algorithm

Chaotic System	Cryptography Algorithm
Sensitive to the initial conditions and control parameters	Diffusion
Iterations	Rounds
Parameters	Key
Set of real numbers	Finite set of integer numbers

Chaos maps can be applied by the use of chaotic systems to generate a pseudorandom key or the generation from a key or plain text. Generation from a pseudorandom key produces a stream cipher and generation from plain text produces a block cipher [13].

3. Chaos-Based General Image Encryption Scheme

Many data encryption methods use chaotic maps [14-20] because it is widely applicable and easy to understand. Chaotic based image encryption occurs in two stages, confusion and diffusion.

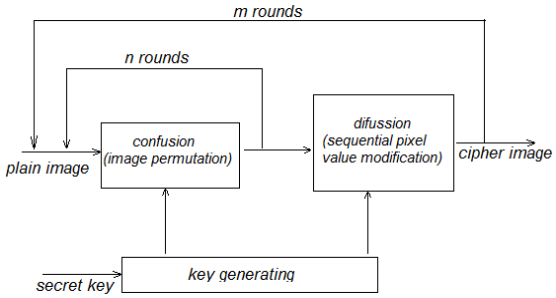

Figure 1. 1Illustrates a Chaos-Based Image Encryption General Scheme

In the confusion stage, an image's pixels are scrambled using a secret key based upon control parameters. While in the diffusion stage, pixel values are changed using chaotically generated sequences. Both these methods make chaotic encryption highly secure [21]. Figure 1 illustrates the chaotic encryption process.

4. Different Chaos-Based Encryption Techniques

[22] Proposed an image-scrambling algorithm that made use of chaotic mapping by encaging each pair of pixels in an image with counterparts in the same image. Pixels are exchanged using a scrambling matrix that is generated from logistic map principles. The proposed algorithm is both simple and efficient. The proposed algorithm was evaluated using a correlation algorithm that indicated the relationship between the degree of scrambling and the scrambling numbers. From our view point the key space of proposed algorithm is not satisfy the security requirement, because it is smaller than the acceptable one. Therefore the transmission of ciphered image will be threatened by brute force attack.

In the algorithm proposed by [23], both a Rössler chaotic system and a Lorenz chaotic system are used for encryption. The use of two or more chaotic systems in an algorithm is highly unusual. Long-term chaotic behavior is periodic and dependent on initial variables [24]. Both of Rössler and Lorenz schemes are each dependent on three variables, make increasing in the security of proposed chaotic system, because of the total parameters number dependent on six variables, making it highly secure. This algorithm shuffles an image's pixels and changes its grayscale values for a set number of iterations before storing the randomized image data in a chaotic matrix the same size as the original image. XOR operations are used for both encryption and decryption. From our view point the key space of the proposed algorithm is good in terms of

increasing the total number of initial parameters to six instead of three for each chaotic system; also the correlation of resulted ciphered image is better.

[25] Proposed an encryption method for colored images using a genetic operator and a chaotic map to minimize the correlation coefficient of adjacent pixels. The proposed algorithm has four steps. First, a logistical map is used to generate four different chaotic sequences by using of four control parameters and four initial values to act as shared keys for the encryption process. Second, quantification, which used to mapped the four sequences into key streams for use in the remaining phases. Third, a crossover used to confuse the image row-by-row and column-by-column. Fourth, a mutation phase used to implement XOR operator between the intermediate image (resulted from crossover stage) and random image. From our view point the proposed image is good in both of correlation coefficient and key space size. Therefore, it highly resist against the brute force attack.

New image encryption scheme based on one of three chaotic systems (Lorenz, Chen or Lu) was proposed by [26] to shuffle the positions of images' pixels by selecting a chaotic system based on a 16-byte key length. Another chaotic system is used to create a chaotic map to disturb the relationship between the encrypted image and the original image. From our view point, the proposed scheme produces large key space and good results in terms of the resulted correlation coefficient.

A new image encryption scheme was proposed by [2] using a combination of W7 and pixel shuffling. A chaotic Henon map is used to generate a permutation matrix using W7 as a secret key and for initial conditions. Pixels shuffling was achieved using horizontal and vertical permutations. Pixel correlations were scattered using a shuffling process. From our view point the proposed scheme has long key space; therefore it is good in brute force resistance. Also it shows good resistance against statistical attack.

A colored image encryption algorithm based on chaotic map and spatial bit-level permutations (SBLP) was proposed by [27]. Image pixel positions were shuffled using a sequence generated from a chaotic logistical map before the shuffled image is transformed into binary matrix. A permutation of the binary matrix is created by scrambling the map generated from the (SBLP) process. A second sequence was generated from a chaotic logistical map to rearrange the new images pixel positions. From our view point, the proposed algorithm is robust against brute force attack because of suitable size of key space also it deal with bit level permutation. Also because of low complexity ant fast implementation time the proposed algorithm can be used in surveillance video systems.

An Enhancement of Advanced Encryption Standard (AES) was proposed by [28]. AES has many drawbacks such as high computational costs, predictable patterns and fixed S-box weak points. The proposed algorithm mitigates these drawbacks using a chaotic map and a XOR operator. The proposed method was tested by using several images and the results show very small correlation coefficients, improved encryption speed and high security. From our view point the proposed algorithm show good adaption for AES algorithm to be implemented in image encryption field.

To reduce the complexity of image encryption, [29] proposed a scheme based on dual-tree complex wavelet transformations (DT-CWT).First stage in this scheme is to transform plain image using wavelet transformation, then a pixel chaotic scrambling is used for approximation and an Arnold transformation is used for the details. From our view point the proposed scheme is suitable, in terms of the key space and correlation coefficient.

An algorithm for generating random bit sequences based on chaotic maps was proposed by [30]. This algorithm uses random bit sequence generated from tent and chaotic logistic maps. The permutation of plain image pixels was done by these chaotic functions, after which the image was divided into eight-bit map planes. Bits were replaced by another bits value according to a chaotic ergodic matrix. From our view point the performance of this algorithm is good in terms of both key sensitivity and key space. Therefore this algorithm is highly resist against brute force attack and statistical attack.

5. Performance Analysis Of Chaotic Cryptography Systems

After Pecora and Carroll discovered synchronization in chaotic systems in 1990 [31], chaotic dynamics has received significant attention due to its use in securing communications

[33-35]. Chaotic signal encoding was first used in 1990 [36]. Some of the most important ways that the strength of chaotic encryption methods has been evaluated are [13], [32]:

5.1. Key Sensitivity Analysis

The use of a secret key for encryption produces strong encryption, as any change in the secret key produces another encrypted image. Secure image cryptosystems makes use of secret keys to evaluate the robustness of an encryption scheme. In a cryptosystem, an image cannot be decrypted if there is any difference between the encryption and decryption keys [37]. In a strong encryption algorithm, key sensitivity should be greater than 50% [38].

5.2. Key Space Analysis

Key space is the number of attempts necessary to guess a correct decryption key. Strong encryption should have an encryption key no smaller than 2^{100} [39], with the exponent indicating the number of bits in a key. Large encryption keys provide greater security against brute force attacks [1].

5.3. Correlation Coefficient Analysis

The correlation coefficient measures similarities between a plain or an encrypted images pixels in the horizontal, vertical and diagonal directions. In a plain image, the correlation coefficient should be high. In an encrypted image, a smaller correlation coefficient indicates higher security [40]. Smaller correlation coefficients are produced from the confusion and diffusion methods.

5.4. Statistical Analysis

Statistical analysis is the most common cryptanalysis technique, and it is used to measure the relationship between a plain image and a ciphered image. Strong cryptographic techniques, when statistically analyzed, show large differences between the plain and ciphered image.

5.5. Image Entropy Analysis

Entropy is used to measure uncertain associations between random variables [41]. A grayscale image has a theoretical entropy value of 8 Sh, or bits. Image encryption algorithms should produce an encrypted image with an entropy value similar to grayscale values [42]. The closer an encrypted images' entropy value is to 8 Sh, the more robust it is against entropy-based attacks.

6. Conclusion

The expansion of the internet and digital communications has increased the need for data protection. The high usage of images for communication means that secure image encryption is necessary. Chaotic based image encryption is one of the best ways to encrypt an image file. In this study, multiple chaotic image encryption methods are discussed and evaluated. Image security can be increased through the application of multiple chaotic image encryption methods.

Acknowledgements

Sabah Fadhel is grateful to the ministry of Sciences and Technology (Baghdad-Iraq), for providing study leave to continue his (Ph. D.).

References

[1] Sankpal, Priya R, PA Vijaya. *Image Encryption Using Chaotic Maps: A Survey. Signal and Image Processing (ICSIP)*. Fifth International Conference on. IEEE, Jan 8 2014: 102-107.
[2] Jolfaei Alireza, AbdolrasoulMirghadri. An image encryption approach using chaos and stream cipher. *Journal of Theoretical and Applied Information Technology*. 2010; 19(2): 117-125.
[3] Wang, Xingyuan, Lin Teng, Xue Qin. A novel colour image encryption algorithm based on chaos. *Signal Processing*. 2012; 92(4): 1101-1108.

[4] Chen, Caisen, Tao Wang, Yingzhan Kou, Xiaocen Chen, Xiong Li. Improvement of trace-driven I-Cache timing attack on the RSA algorithm. *Journal of Systems and Software*. 2013; 86(1): 100-107.
[5] Coppersmith Don. The Data Encryption Standard (DES) and its strength against attacks. *IBM Journal of Research and Development*. 1994; 38(3): 243-250.
[6] Bashardoost, Morteza, MohdShafryMohd Rahim, Ayman Altameem, Amjad Rehman. A Novel Approach to Enhance the Security of the LSB Image Steganography. *Research Journal of Applied Sciences, Engineering and Technology*. 2014; 7(19): 3957-3963.
[7] Jain A. Pixel chaotic shuffling and Arnold map based Image Security Using Complex Wavelet Transform. *Journal of Network Communications and Emerging Technologies (JNCET)*. 2016; 6(5): 8-11.
[8] Liu, Shubo, Jing Sun, ZhengquanXu. An improved image encryption algorithm based on chaotic system. *Journal of Computers*. 2009; 4(11): 1091-1100.
[9] Alsafasfeh, Qais H, Aouda A. Arfoa. Image encryption based on the general approach for multiple chaotic systems. *Journal of Intelligent Learning Systems and Applications*. 2011; 3(3): 238-244.
[10] Liu, Lingfeng, Suoxia Miao. A new image encryption algorithm based on logistic chaotic map with varying parameter. *SpringerPlus*. 2016; 5(1): 1.
[11] Priya R. Sankpal, PA Vijaya. *Image Encryption Using Chaotic Maps: A Survey*. In Signal and Image Processing (ICSIP), 2014 Fifth International Conference. 2014: 102-107.
[12] Somaya Al-Maadeed, Afnan Al-Ali, Turki Abdalla. A new chaos-based image-encryption and compression algorithm. *Journal of Electrical and computer Engineering*. 2012: 15.
[13] Ali Soleymani, ZulkarnainMd Ali, Md Jan Nordin. A survey on principal aspects of secure image transmission. World Academy of Science, Engineering and Technology. 2012; 66.
[14] ToshikiHabutsu, Yoshifumi Nishio, Iwao Sasase, Shinsaku Mori. *A secret key cryptosystem by iterating a chaotic map*. In Workshop on the Theory and Application of Cryptographic Techniques. Springer Berlin Heidelberg: 1991: 127-140.
[15] Franz Pichler, Josef Scharinger. *Finite dimensional generalized baker dynamical systems for cryptographic applications*. In International Conference on Computer Aided Systems Theory. Springer Berlin Heidelberg: 1995: 465-476.
[16] Naoki Masuda, Kazuyuki Aihar. Cryptosystems with discretized chaotic maps. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*. 2002; 49(1): 28-40.
[17] J-C, Yeo, J-I Guo. Efficient hierarchical chaotic image encryption algorithm and its VLSI realisation. *IEE Proceedings-vision, image and signal processing*. 2000; 147(2): 167-175.
[18] Yen JC, Guo JI. *A new chaotic key-based design for image encryption and decryption*. ISCAS, IEEE International Symposium on Circuits and Systems. 2000; 4: 49-52.
[19] Chen Guanrong, Yaobin Mao, Charles K Chui. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals.* 2004; 21(3): 749-761.
[20] ShiguoLian, Jinsheng Sun, Zhiquan Wang. Security analysis of a chaos-based image encryption algorithm. *Physica A: Statistical Mechanics and its Applications*. 2005; 351(2): 645-661.
[21] Image Encryption and Decryption of Digital Color Images. *International Journal of information and Education Technology*. June 2011; 1(2): 137.
[22] Yupu Dong, Jiasheng Liu, Canyan Zhu, Yiming Wang. *Image encryption algorithm based on chaotic mapping*. (ICCSIT), 2010 3rd IEEE International Conference. 2010; 1: 289-291.
[23] Qais H Alsafasfeh, Aouda A Arfoa. Image encryption based on the general approach for multiple chaotic systems. *Journal of Intelligent Learning Systems and Applications*. 2011; 3(3): 238-244.
[24] Ling Wang, Qun Ye, Yaoqiang Xiao, YongxingZou, Bo Zhang. *An image encryption scheme based on cross chaotic map*. Congress onImage and Signal Processing. 2008; 3: 22-26.
[25] ES El-Alfy, K Al-Utaibi. *An Encryption Scheme for Color Images Based on Chaotic Maps and Genetic Operators*. The Seventh International Conference on Networking and Services. 2011: 92-97.
[26] K Sakthidasan, BV Santhosh Krishna. A new chaotic algorithm for image encryption and decryption of digital color images. *International Journal of Information and Education Technology*. 2011; 1(2): 137-141.
[27] Rui Liu, Xiaoping Tian. New Algorithm for Color Image Encryption Using Chaotic Map and Spatial Bit-Level Permutation. *Journal of Theoretical & Applied Information Technology*. 2012; 43(1): 89-93.
[28] Ali Abdulgader, Mahamod Ismail, Nasharuddin Zainal, TarikIdbeaa. Enhancement of AES algorithm based on chaotic maps and shift operation for image encryption. *Journal of Theoretical and Applied Information Technology*. 2015; 71(1): 1-12.
[29] Abhinav Jain, ArjunVerma. Pixel chaotic shuffling and Arnold map based Image Security Using Complex Wavelet Transform. *Journal of Network Communications and Emerging Technologies (JNCET)*. 2016; 6(5): pp. 8-11.
[30] HimanKhanzadi, Mohammad Eshghi, ShahramEtemadiBorujeni. Image encryption using random bit sequence based on chaotic maps. *Arabian Journal for Science and engineering*. 2014; 39(2): 1039-1047.
[31] Pecora, Louis M, Thomas L Carroll. Synchronization in chaotic systems. Physical review letters. 1990; 64(8): 821.

[32] D Chattopadhyay, MK Mandal, D Nandi. Symmetric key chaotic image encryption using circle map. *Indian Journal of Science and Technology*. 2011; 4(5): 593-599.
[33] Gonzalo Alvarez, Shujun Li. Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*. 2006; 16(8): 2129-2151.
[34] L Gámez-Guzmán, C Cruz-Hernández, RM López-Gutiérrez, EE. Garcia-Guerrero. Synchronization of multi-scroll chaos generators: application to private communication*. Revistamexicana de física*. 2008; 54(4): 299-305.
[35] L Gámez-Guzmán, C Cruz-Hernández, RM López-Gutiérrez, EE García-Guerrero. Synchronization of Chua's circuits with multi-scroll attractors: application to communication. Communications in Nonlinear Science and Numerical Simulation. 2009; 14(6): 2765-2775.
[36] César Cruz-Hernández, Didier López-Mancilla, V García-Gradilla, H Serrano-Guerrero, R Núñez-Pérez. Experimental realization of binary signals transmission using chaos. *Journal of Circuits, Systems, and Computers*. 2005; 14(3): 453-468.
[37] Belmeguenaï Aïssa, Derouiche Nadir, Redjimi Mohamed. Image encryption using stream cipher based on nonlinear combination generator with enhanced security. *New Trends in Mathematical Sciences*. 2013; 1(1): 10-19.
[38] Ali ShakirMahmood, MohdShafryMohd Rahim, NurZuraifahSyazrah Othman. Implementation of the Binary Random Number Generator Using the Knight Tour Problem. *Modern Applied Science*. 2016; 10(4): 35-46.
[39] Narendra K Pareek. Design and analysis of a novel digital image encryption scheme. *International Journal of Network Security & Its Applications (IJNSA).* March 2012; 4(2): 95-108.
[40] Mohit Kumar, AnjuChahal. Effect of Encryption Technique and Size of Image on Correlation Coefficient in Encrypted Image*. International Journal of Computer Applications*. 2014; 97(12): 23-27.
[41] Jamal N BaniSalameh, PO Mu'tah–Karak. An Investigation of the Use of MJEA in Image Encryption. *WSEAS TRANSACTIONS on COMPUTERS*. 2016; 15: 12-23.
[42] T Sivakumar, R Venkatesan. A New Image Encryption Method Based on Knight's Travel Path and True Random Number. *Journal of Information Science and Engineering*. 2016; 32(1): 133-152.

BIOGRAPHIES OF AUTHORS

Sabah Fadhel Hamood
1. B. Sc. Physics Science – Al-Nahrain University / Baghdad – Iraq (1995)
2. High Diploma. Computer Since– National Computer Center / Baghdad Iraq(1999)
3. M. Sc. Computer Science – (UTM) / Johor Malaysia (2013)

Dr.Mohd Shafry Mohd Rahim
1. Ph.D (Spatial Modeling) (UPM)
2. M. Comp. Sci. (UTM)
3. B. Comp. Sci. (Computer Graphics) (UTM)
4. Dip. Comp. Sc. (UTM)

Omar FarookMohammado
1. B. Sc. Computer Science – University of Mosul / Mosul – Iraq (2005)
2. M. Sc. Computer Sciences – Hamdard University / New Delhi – India (2011)